Information and Computation **151**, 32–56 (1999)
Article ID inco.1998.2763, available online at http://www.idealibrary.com on IDEAL®

# On Cryptographic Propagation Criteria for



Claude Carlet

*GREYC, Université de Caen and INRIA Projet Codes, Domaine de Voluceau, BP 105, 78153 Le Chesnay Cedex, France*
E-mail: Claude.Carlet@inria.fr*

We determine the functions on $GF(2)^n$ which satisfy the propagation criterion of degree $n-2$, $PC(n-2)$. We study subsequently the propagation criterion of degree $\ell$ and order $k$ and its extended version $EPC$. We determine those Boolean functions on $GF(2)^n$ which satisfy $PC(\ell)$ of order $k \geqslant n-\ell-2$. We show that none of them satisfies $EPC(\ell)$ of the same order. We finally give a general construction of nonquadratic functions satisfying $EPC(\ell)$ of order $k$. This construction uses the existence of nonlinear, systematic codes with good minimum distances and dual distances (e.g., Kerdock codes and Preparata codes). 

## 1. INTRODUCTION

Let $n$ be a positive integer. The *bent* functions [11, 16, 28] are those Boolean functions on $GF(2)^n$ whose Hamming distance[1] to the Reed–Muller code of order 1 (the set of all affine functions on $GF(2)^n$) is equal to the covering radius of this code, i.e., is optimum. In other words, their nonlinearity is maximum, from the viewpoint of Hamming distance.

The covering radius of the Reed–Muller code of order 1 is known and equal to $2^{n-1}-2^{n/2-1}$ for any even $n$. It is unknown for any odd $n \geqslant 9$.

The bent functions on $GF(2)^n$ with $n$ even have extra properties which make them very interesting from cryptographic viewpoint. They are called *perfect nonlinear* [24] and are characterized by the following equivalent facts:

1. for any word $a \in GF(2)^n$, the value at $a$ of the Walsh transform of the real-valued function $f_\chi(x) = (-1)^{f(x)}$ (i.e., the discrete Fourier transform of function $f$) $\widehat{f_\chi}(a) = \sum_{x \in GF(2)^n} (-1)^{f(x)+x\cdot a}$ is equal to $\pm 2^{n/2}$ ("$\cdot$" denotes the usual dot product on $GF(2)^n$);

2. the support $\{x \in GF(2)^n \mid f(x)=1\}$ is a difference set;

* www: http://www.info.unicaen.fr/~claude/english.html.

[1] The Hamming distance between two Boolean functions is equal to the number of words in $GF(2)^n$ at which their values differ.



0890-5401/99 $30.00

3. for any nonzero word $a$, the Boolean function $f(x)+f(x+a)$ is balanced (i.e., takes the values 0 and 1 equally often; the addition is in $GF(2)$).

The set of bent functions has the following properties of stability: for any $n$, the automorphism group of the Reed–Muller code of order 1 being the general affine group, the set of bent functions is globally invariant under the action of this group; it is also invariant under the addition of any affine function; finally, if $f$ is perfect nonlinear, then the Boolean function $\tilde{f}$ defined by

$$\widehat{f_\chi}(a) = 2^{n/2}(-1)^{\tilde{f}(a)}; \qquad a \in GF(2)^n,$$

is perfect nonlinear as well; it is called the *dual* of $f$ (the dual of $\tilde{f}$ is $f$ itself).

The quadratic perfect nonlinear functions are the functions

$$f(x) = \sum_{1 \leqslant i < j \leqslant n} a_{i,j} x_i x_j + h(x) \qquad (h \text{ affine}, a_{i,j} \in F_2)$$

whose associated symplectic forms, $\varphi_f$: $(x, y) \mapsto f(0)+f(x)+f(y)+f(x+y)$ are nondegenerate (cf. [29]).

Perfect nonlinear functions have a cryptographic drawback; they are not balanced.[2] This has led Bart Preneel to the introduction of a hierarchy on Boolean functions, whose highest level is that of perfect nonlinear functions, where we find balanced functions at lower levels: for any positive integers $n$ and $\ell$, a Boolean function $f$ on $GF(2)^n$ satisfies the *propagation criterion* $PC(\ell)$ *of degree* $\ell$ (cf. [25]), if $f(x)$ changes with a probability $\frac{1}{2}$ whenever at least one and at most $\ell$ coordinates of $x$ are complemented. In other words, $f$ satisfies $PC(\ell)$ if, for any nonzero word $a$ of Hamming weight $\omega(a) \leqslant \ell$, the Boolean function $f(x)+f(x+a)$ is balanced. The third characterization of perfect nonlinear functions given above is equivalent to saying that the perfect nonlinear functions on $GF(2)^n$ are those Boolean functions which satisfy the propagation criterion of any degree (i.e., of degree $n$).

The set of those functions which satisfy $PC(\ell)$ is globally invariant under the composition with any permutation of the coordinates $x_1, ..., x_n$, the complementation of any of these coordinates, and the addition of any affine function. PC(1) is called the *strict avalanche criterion SAC*.

We need, for cryptographic purpose, to use Boolean functions which satisfy $PC(\ell)$ when we keep constant a certain number $k$ of their coordinates (whatever these coordinates are and whatever the constant values chosen for them are). These functions are said to satisfy the *propagation criterion* $PC(\ell)$ *of order* $k$ (cf. [25–26, 27]). The set of functions which satisfy this criterion is globally invariant under the same transformations as in the case of $PC(\ell)$. The *strict avalanche criterion of order* $k$, $SAC(k)$ is by definition the same as $PC(1)$ of order $k$.

A stronger notion, also introduced by Bart Preneel (cf. [25, 27]), is that of the *extended propagation criterion* $EPC(\ell)$ *of order* $k$: a function $f$ satisfies $EPC(\ell)$ of order $k \leqslant n-\ell$ if the knowledge of $k$ coordinates of $x$ gives no information on the

[2] Practically, this is a drawback for small values of $n$ only, for $n \geqslant 20$, the difference $2^{n/2-1}$ between the weight of a perfect nonlinear function and the weight $2^{n-1}$ of balanced functions is negligible.

values of the functions $f(x)+f(x+a)$, $1 \leqslant \omega(a) \leqslant \ell$. The set of those functions which satisfy this criterion is globally invariant under the same transformations as in the case of $PC(\ell)$.

Every Boolean function $f$ on $GF(2)^n$ admits a unique algebraic normal form (cf. [29]),

$$f(x_1, ..., x_n) = \sum_{u \in GF(2)^n} a_u \left( \prod_{i=1}^{n} x_i^{u_i} \right),$$

where $a_u \in GF(2)$ for every $u \in GF(2)^n$. We call the algebraic *degree* of $f$ the (global) degree of this algebraic normal form. Bart Preneel gives in [25] an upper bound on the degree of any $SAC(k)$ function (and, therefore, of any function satisfying $PC(\ell)$ of order $k$ with $\ell \geqslant 1$). The degree of such a function is bounded by $n-k-1$ if $k < n-2$ and equal to 2 if $k = n-2$; the case $k=0$ comes simply from the more general fact that, if at least one of the functions $f(x)+f(x+a)$, $a \neq 0$ is balanced, and if $n > 2$ then $f$ must have an even weight, i.e., have degree smaller than or equal to $n-1$. The case $k > 0$ follows straightforwardly. There does not exist any more precise known bound on the degree of those Boolean functions which satisfy $PC(\ell)$ of order $k$ for $\ell > 1$ (except when $\ell + k \geqslant n$, since we know that any perfect non-linear function on $GF(2)^\ell$, $\ell$ even $\geqslant 4$ has degree smaller than or equal to $\ell/2$; but we will see below that, in this case, the degree of $f$ is in fact equal to 2).

The first purpose of this paper is to determine those functions which satisfy the propagation criterion of degree $\ell$ and high order. We shall determine in Section 4 the functions satisfying $PC(\ell)$ of orders greater than or equal to $n-\ell-2$ and show that none of them satisfies $EPC(\ell)$ of the same order. To obtain such a result, we need to describe in Section 3 those functions which satisfy $PC(n-1)$ and $PC(n-2)$. The main results were already given in [10], but some of them without proofs.

If a function $f$ satisfies $PC(\ell)$ of order $k \leqslant n-\ell$, then it satisfies $PC(\ell)$ of order $k'$ for any $k' \leqslant k$ (cf. Proposition 2). Thus, $PC(\ell)$ of order $k$ is a stronger condition than $PC(\ell)$ (i.e., $PC(\ell)$ of order 0). It is actually more difficult to satisfy, even for small values of $k$. Kurosawa and Satoh [23] give a nice general method to design functions satisfying $PC(\ell)$ (in fact, $EPC(\ell)$, but they do not notice this) of order $k$. But, as we explain it in Subsection 5.1, the functions they obtain have a peculiarity which weakens them. We show that the generalization of their construction given in [10] leads to functions satisfying $EPC(\ell)$ of order $k$, and we study in detail the other cryptographic properties of the functions obtained this way.

## 2. PRELIMINARIES

We first give a characterization that will be useful in the sequel.

### 2.1. A Characterization of the Criterion $PC(\ell)$

*Notation.* For any binary vectors $u$ and $v$ of length $n$, we write $v \preccurlyeq u$ if the support of $u$ contains that of $v$. We denote by $\bar{u}$ the word $(u_1+1, ..., u_n+1)$ and by $\omega(u)$ the Hamming weight of $u$.

PROPOSITION 1. *Let $0 \leqslant \ell \leqslant n$. Any Boolean function $f$ on $GF(2)^n$ satisfies $PC(\ell)$ if and only if, for every word $u$ of weight $\ell$ and every word $v$:*

$$\sum_{w \preccurlyeq \bar{u}} \widehat{f_\chi}^2(w+v) = 2^{\omega(\bar{u})+n}.$$

*Proof.* For every function $f$ and any words $u$ and $v$, we have

$$\begin{aligned}
\sum_{w \preccurlyeq \bar{u}} \widehat{f_\chi}^2(w+v) &= \sum_{w \preccurlyeq \bar{u}} \left( \sum_{x \in GF(2)^n} (-1)^{f(x)+x\cdot(w+v)} \right)^2 \\
&= \sum_{w \preccurlyeq \bar{u}} \left( \sum_{x,\, y \in GF(2)^n} (-1)^{f(x)+f(y)+(x+y)\cdot(w+v)} \right) \\
&= \sum_{x,\, y \in GF(2)^n} \left( (-1)^{f(x)+f(y)+(x+y)\cdot v} \sum_{w \preccurlyeq \bar{u}} (-1)^{(x+y)\cdot w} \right) \\
&= 2^{\omega(\bar{u})} \sum_{x,\, y \in GF(2)^n \mid x+y \preccurlyeq u} (-1)^{f(x)+f(y)+(x+y)\cdot v} \\
&= 2^{\omega(\bar{u})} \sum_{s \preccurlyeq u} \left( (-1)^{s\cdot v} \sum_{x \in GF(2)^n} (-1)^{f(x)+f(x+s)} \right).
\end{aligned}$$

$f$ satisfies $PC(\ell)$ if and only if, for every word $u$ of weight $\ell$, the autocorrelation function $s \mapsto \sum_{x \in GF(2)^n} (-1)^{f(x)+f(x+s)}$ takes the value 0 at every nonzero element of the set $\{s \in GF(2)^n \mid s \preccurlyeq u\}$. The value at 0 of the autocorrelation function of any Boolean function being equal to $2^n$, this is equivalent to the fact that the Walsh transform of the restriction to such set of this autocorrelation function, i.e., the sum:

$$\sum_{s \preccurlyeq u} \left( (-1)^{s\cdot v} \sum_{x \in GF(2)^n} (-1)^{f(x)+f(x+s)} \right),$$

is equal to $2^n$. This proves the equivalence. ∎

*Remarks.* 1. The condition "$u$ of weight $\ell$" can be replaced by "$u$ of weight smaller than or equal to $\ell$" in the statement of Proposition 1.

2. For $\ell = 0$, we obtain Parseval's relation, which is actually valid for every Boolean function.

### *2.2. Generalities on the Criteria $PC(\ell)$ and $EPC(\ell)$ of Order $k$*

In his original definition, Preneel imposes *a priori* that $k$ is smaller than or equal to $n-\ell$. This restriction is not absolutely necessary. But, clearly, if a function $f$ on $GF(2)^n$ satisfies the propagation criterion of degree $\ell$ and order $n-\ell$, then it satisfies $PC(\ell')$ of order $n-\ell$ for every $\ell'$. Notice that $\ell$ must then be even, since any restriction of $f$ obtained by keeping constant $n-\ell$ coordinates must be perfect nonlinear.

By definition, if a function $f$ satisfies $EPC(\ell)$ of order $k \leqslant n-\ell$, then it satisfies $EPC(\ell)$ of order $k'$ for any $k' \leqslant k$. Similarly,

PROPOSITION 2. *If a function $f$ satisfies $PC(\ell)$ of order $k \leqslant n-\ell$, then it satisfies $PC(\ell)$ of order $k'$ for any $k' \leqslant k$.*

*Proof.* To check this, it is enough to consider the case $k' = k-1$. Let $f'$ be the restriction of $f$ obtained by keeping constant $k-1$ coordinates—say the last $(k-1)$ ones. Let $a \in GF(2)^{n-k+1}$ have weight at most $\ell$. Since $\ell \leqslant n-k$, there exists $i \leqslant n-k+1$ such that $a_i = 0$. Both restrictions of the function $f'(x) + f'(x+a)$ obtained by keeping $x_i$ constant are then balanced, since $f'$ satisfies $PC(\ell)$ of order 1. This implies that the function $f'(x) + f'(x+a)$ itself is balanced. ▮

The definition of the extended propagation criterion is closely related to the notion of resilient function:

DEFINITION 1. A function $f$ from $GF(2)^n$ to $GF(2)^m$ is $k$th order correlation-immune if the probability distribution of the values of $f(x_1, ..., x_n)$, where $x_1, ..., x_n$ are considered as random input variables assuming values from $GF(2)$ with independent equiprobable distributions, is unaltered when at most $k$ of the coordinates $x_1, ..., x_n$ are kept constant. It is $k$-resilient if it is balanced (i.e., takes all the values in $GF(2)^m$ equally often) and $k$th order correlation-immune.

PROPOSITION 3 [27]. *A Boolean function $f$ satisfies the* extended propagation criterion *$EPC(\ell)$ of order $k$, if and only if, for any nonzero word $a$ of Hamming weight smaller than or equal to $\ell$, the Boolean function $f(x) + f(x+a)$ is $k$-resilient.*

*Remark.* We know (cf. [33]) that the algebraic degree of any $k$-resilient Boolean function on $GF(2)^n$ is smaller than or equal to $n-k-1$ if $k \leqslant n-2$ and equal to 1 if $k = n-1$. This leads to a bound on the degree of the functions satisfying $EPC(\ell)$ of order $k$ ($\ell \geqslant 1$). Let $f$ be such function; write for every $i \in \{1, ..., n\}$:

$$f(x_1, ..., x_n) = g_i(x_1, ..., x_{i-1}, x_{i+1}, ..., x_n) + x_i h_i(x_1, ..., x_{i-1}, x_{i+1}, ..., x_n).$$

Denote by $e_i$ the word of weight 1 whose $i$th coordinate is equal to 1; we have $h_i(x_1, ..., x_{i-1}, x_{i+1}, ..., x_n) = f(x) + f(x+e_i)$. Thus, $h_i$ is $k$-resilient and its degree is therefore smaller than or equal to $n-k-2$ if $k \leqslant n-3$ and equal to 1 if $k = n-2$. This implies that $f$ has degree smaller than or equal to $n-k-1$ if $k \leqslant n-3$ and equal to 2 if $k = n-2$. Unfortunately, this is nothing more than Preneel's bound, recalled in the Introduction.

There exists a characterization of resilient functions in terms of their Fourier transform. We recall it in the case of a Boolean function only. The general characterization can be found in [4] but will not be used in this paper.

LEMMA 1 [33]. *A Boolean function $f$ on $GF(2)^n$ is $k$th order correlation-immune (resp. $k$-resilient) if and only if, for every word $b$ such that $1 \leqslant \omega(b) \leqslant k$ (resp. $\omega(b) \leqslant k$):*

$$\sum_{x \in GF(2)^n} (-1)^{f(x) + b \cdot x} = 0.$$

Two characterizations were given by Preneel [27].

PROPOSITION 4 [27]. *A function $f$ satisfies $EPC(\ell)$ (resp. $PC(\ell)$) of order $k$ if and only if, for any word $a$ of Hamming weight smaller than or equal to $\ell$ and any word $b$ of Hamming weight smaller than or equal to $k$, if $(a, b) \neq (0, 0)$ (resp. if $(a, b) \neq (0, 0)$ and if $a$ and $b$ have disjoint supports) then*:

$$\sum_{x \in GF(2)^n} (-1)^{f(x)+f(x+a)+b\cdot x} = 0.$$

We deduce the following property which will be useful in the sequel.

PROPOSITION 5. *Let $f$ be any perfect nonlinear function. Let $\ell$ and $k$ be any nonnegative integers. Then $f$ satisfies $PC(\ell)$ of order $k$ (resp. $EPC(\ell)$ of order $k$) if and only if its dual $\tilde{f}$ satisfies $PC(k)$ of order $\ell$ (resp. $EPC(k)$ of order $\ell$).*

This is a direct consequence of Proposition 4 and of the following.

LEMMA 2. *Let $f$ be any perfect nonlinear function on $GF(2)^n$ ($n$ even $\geqslant 2$) and $\tilde{f}$ its dual. Let $a$ and $b$ be two words in $GF(2)^n$. Then,*

$$\sum_{x \in GF(2)^n} (-1)^{f(x)+f(x+a)+b\cdot x} = \sum_{y \in GF(2)^n} (-1)^{\tilde{f}(y)+\tilde{f}(y+b)+a\cdot y}.$$

*Proof.* By definition of $\tilde{f}$, we have

$$\begin{aligned}
&\sum_{y \in GF(2)^n} (-1)^{\tilde{f}(y)+\tilde{f}(y+b)+a\cdot y} \\
&\quad = 2^{-n} \sum_{y \in GF(2)^n} \left( \sum_{x,\, x' \in GF(2)^n} (-1)^{f(x')+f(x)+x'\cdot y+x\cdot(y+b)+a\cdot y} \right) \\
&\quad = 2^{-n} \sum_{x,\, x' \in GF(2)^n} \left( (-1)^{f(x)+f(x')+x\cdot b} \sum_{y \in GF(2)^n} (-1)^{(x+x'+a)\cdot y} \right).
\end{aligned}$$

We know that all the sums $\sum_{y \in GF(2)^n} (-1)^{u\cdot y}$, $u \neq 0$, are equal to 0. We deduce:

$$\sum_{y \in GF(2)^n} (-1)^{\tilde{f}(y)+\tilde{f}(y+b)+a\cdot y} = \sum_{x \in GF(2)^n} (-1)^{f(x)+f(x+a)+x\cdot b}. \quad \blacksquare$$

## 3. FUNCTIONS SATISFYING THE PROPAGATION CRITERION OF DEGREE GREATER THAN OR EQUAL TO $n-2$

We shall use the known lemma in the sequel.

LEMMA 3 [19]. *Let $a$, $b$, $c$, and $d$ be four nonnegative integers. Assume that $a^2+b^2+c^2+d^2 = 2^m$, then*:

— *if $m$ is even $\geqslant 2$, then either one integer among $a$, $b$, $c$ and $d$ is equal to $2^{m/2}$ and all the others are equal to 0, or $a = b = c = d = 2^{m/2-1}$;*

— *if $m$ is odd, then two among these integers are equal to $2^{(m-1)/2}$ and the two others are equal to 0.*

The proof is straightforward by induction on $m$ (by using the fact that the sum of the squares of four integers which are not all even cannot be divisible by 8).

The functions which satisfy the propagation criterion of degree $n-2$ have been characterized by Hirose and Ikeda in a technical report (cf. [19]). We give in Proposition 6 the complete description of these functions, which is not given in [19]. We give also an original and simpler proof of this proposition.

PROPOSITION 6. *Let $n$ be even $\geqslant 4$. The only Boolean functions on $GF(2)^n$ which satisfy $PC(n-2)$ are the perfect nonlinear functions (i.e., satisfy $PC(n)$). Let $n$ be odd $\geqslant 3$. The Boolean functions which satisfy $PC(n-1)$ are the functions of the form*

$$f(x_1, ..., x_n) = g(x_1 + x_n, ..., x_{n-1} + x_n) + h(x_1, ..., x_n) \tag{1}$$

*where $g$ is any perfect nonlinear function on $GF(2)^{n-1}$ and $h$ is any affine function on $GF(2)^n$. The functions which satisfy $PC(n-2)$ are the functions $f(x_1, ..., x_n)$ of the form (1) and those of the two forms,*

$$g(x_1 + x_n, ..., x_{i-1} + x_n, x_i, x_{i+1} + x_n, ..., x_{n-1} + x_n) + h(x_1, ..., x_n) \tag{2}$$

$$g(x_1 + x_{n-1}, ..., x_{n-2} + x_{n-1}, x_n) + h(x_1, ..., x_n) \tag{3}$$

*where $g$ and $h$ are as above. Equivalently, for odd $n \geqslant 3$, the functions which satisfy $PC(n-2)$ are those functions $f$ for which:*

(i) *there exists a nonzero word $a$ of Hamming weight $\omega(a) \geqslant n-1$ such that the function $f(x) + f(x+a)$ is constant,*

(ii) *for every nonzero word $b \neq a$, the function $f(x) + f(x+b)$ is balanced on $GF(2)^n$.*

Thus, as described by Hirose and Ikeda, any function satisfying $PC(n-2)$ admits one linear structure $a$ and one only. This linear structure has weight $n-1$ or $n$. Notice that the functions of the forms (1), (2), and (3) are all partially bent (cf. [7]). They are linearly equivalent to $g(x_1, ..., x_{n-1})$ or to $g(x_1, ..., x_{n-1}) + x_n$, and we know that the set of partially bent functions is globally invariant under any linear permutation on $GF(2)^n$.

*Proof.* If $n$ is odd, all the functions satisfying (1), (2), or (3) satisfy (i) and (ii), $g$ being perfect nonlinear. Thus, they satisfy $PC(n-2)$. If $n$ is even, any perfect nonlinear function satisfies $PC(n-2)$. Let us show that the converse is also true in both cases. According to Proposition 1, for every word $u$ of weight $n-2$, every word $v$, and every function $f$ satisfying $PC(n-2)$:

$$\sum_{w \preccurlyeq \bar{u}} \widehat{f_\chi}^2(w+v) = 2^{n+2}.$$

In other words, for every indices $i \neq j$ and every word $v$, we have

$$\widehat{f_\chi}^2(v) + \widehat{f_\chi}^2(v+e_i) + \widehat{f_\chi}^2(v+e_j) + \widehat{f_\chi}^2(v+e_i+e_j) = 2^{n+2}. \tag{4}$$

Assume first that $n$ is even. According to Lemma 3, for every $v$:

1. either one of the integers $\widehat{f_\chi}(v), \widehat{f_\chi}(v+e_i), \widehat{f_\chi}(v+e_j), \widehat{f_\chi}(v+e_i+e_j)$ is equal to $\pm 2^{n/2+1}$ and the others are all equal to 0;
2. or they are all equal to $\pm 2^{n/2}$.

Suppose that one of the numbers $\widehat{f_\chi}(v)$, $v \in GF(2)^n$ is equal to $\pm 2^{n/2+1}$. Then, for every word $w$ of weight one or two, $\widehat{f_\chi}(v+w)$ is equal to 0. Thus, for every word of weight three, $w = e_i + e_j + e_k$, $\widehat{f_\chi}(v+w)$ is equal to $\pm 2^{n/2+1}$ (apply Lemma 3 to relation (4), where $v$ is replaced by $v+e_k$). We deduce that if $n \geqslant 4$ and if $i, j, k, k'$ are four different indices, $\widehat{f_\chi}(v+e_i+e_j+e_k)$ and $\widehat{f_\chi}(v+e_i+e_j+e_{k'})$ are both equal to $\pm 2^{n/2+1}$, a contradiction, since $\widehat{f_\chi}^2(v+e_i+e_j+e_k)+\widehat{f_\chi}^2(v+e_i+e_j)+\widehat{f_\chi}^2(v+e_i+e_j+e_k+e_{k'})+\widehat{f_\chi}^2(v+e_i+e_j+e_{k'})$ would be greater than or equal to $2^{n+3}$. Thus, every number $\widehat{f_\chi}(v)$ is equal to $\pm 2^{n/2}$ and $f$ is perfect nonlinear.

Assume now that $n$ is odd. Let $f$ be a function satisfying $PC(n-2)$. According to Lemma 3, for every $v$, two among the integers $\widehat{f_\chi}(v)$, $\widehat{f_\chi}(v+e_i)$, $\widehat{f_\chi}(v+e_j)$, $\widehat{f_\chi}(v+e_i+e_j)$ are equal to $\pm 2^{(n+1)/2}$ and the two others are equal to 0.

Assume that $\widehat{f_\chi}(v)$ and $\widehat{f_\chi}(v+e_i)$ are equal to $\pm 2^{(n+1)/2}$ for some $v \in GF(2)^n$ and some $i = 1, ..., n$. We can without loss of generality assume that $v = 0$ (otherwise, we change $f(x)$ into $f(x)+v \cdot x$). Then, we deduce by induction on the weight of $w$ that for every word $w$ such that $w_i = 0$, the numbers $\widehat{f_\chi}(w)$ and $\widehat{f_\chi}(w+e_i)$ are equal to $\pm 2^{(n+1)/2}$ if $w$ has an even weight and they are equal to 0 otherwise.

We assume first that $i < n$. Let $E_i = \{ w \in GF(2)^n \mid \sum_{j \neq i} w_j = 0 \}$. We have

$$\widehat{f_\chi}(w) = 0, \quad \forall w \notin E_i, \qquad \widehat{f_\chi}(w) = \pm 2^{(n+1)/2}, \quad \forall w \in E_i.$$

Thus, for every $u$ in $GF(2)^n$, according to the inverse Fourier formula,

$$f_\chi(u) = 2^{-n} \sum_{w \in GF(2)^n} \widehat{f_\chi}(w)(-1)^{w \cdot u} = 2^{-n} \sum_{w \in E_i} \widehat{f_\chi}(w)(-1)^{w \cdot u}.$$

Every element of $E_i$ can be written in the form $(w', h_i(w'))$, where $w' = (w'_1, ..., w'_{n-1}) \in GF(2)^{n-1}$ and $h_i(w') = \sum_{j \neq i} w'_j$. We deduce

$$f_\chi(u) = 2^{-n} \sum_{w' \in GF(2)^{n-1}} \widehat{f_\chi}(w', h_i(w'))(-1)^{w' \cdot u' + u_n h_i(w')}$$

where $u' = (u_1, ..., u_{n-1})$;

$$f_\chi(u) = 2^{-n} \sum_{w' \in GF(2)^{n-1}} \widehat{f_\chi}(w', h_i(w'))(-1)^{w' \cdot (u' + u_n \overline{e'_i})}$$

where $e'_i$ is the word of length $n-1$ and weight 1 whose $i$th coordinate is equal to 1. Therefore, there exists $g$ such that $f(u) = g(u' + u_n \overline{e'_i})$. To complete this case, let us show that $g$ is perfect nonlinear, i.e., that $f$ has the form (2). Suppose there exists a nonzero word $a'$ of length $n-1$ such that $g(x)+g(x+a')$ is not balanced. The functions $f(x)+f(x+(a',0))$ and $f(x)+f(x+(a'+\overline{e'_i},1))$ are also not balanced. Thus, the words $(a',0)$ and $(a'+\overline{e'_i},1)$ have weight greater than or equal to $n-1$,

a contradiction if $n \geqslant 5$. If $n = 3$, then $g$ is quadratic nonaffine; it is therefore perfect nonlinear, since it is defined on $GF(2)^2$.

The case where $i = n$ follows by exchanging $n$ with $n-1$ in relation (2) with $i = n-1$. We obtain then the functions of the form (3).

To check that any function satisfying $PC(n-2)$ must have one of the forms (1), (2), or (3), the last case to consider is when there does not exist any $v$ and $i$ such that $\widehat{f_\chi}(v)$ and $\widehat{f_\chi}(v+e_i)$ are equal to $\pm 2^{(n+1)/2}$. Choose $v$ such that $\widehat{f_\chi}(v) = \pm 2^{(n+1)/2}$. We can without loss of generality assume that $v = 0$. Then for every $i$, we have $\widehat{f_\chi}(e_i) = 0$. We deduce by induction on the weight of $w$ that for every $w$, $\widehat{f_\chi}(w)$ is equal to $\pm 2^{(n+1)/2}$ if $w$ has an even weight, and to 0 otherwise. Let $E = \{w \in GF(2)^n \mid \sum_{i=1}^n w_i = 0\}$. We have, for every $u$ in $GF(2)^n$,

$$\begin{aligned} f_\chi(u) &= 2^{-n} \sum_{w \in E} \widehat{f_\chi}(w)(-1)^{w \cdot u} \\ &= 2^{-n} \sum_{w' \in GF(2)^{n-1}} \widehat{f_\chi}(w', h(w'))(-1)^{w' \cdot u' + u_n h(w')}, \end{aligned}$$

where $h(w') = \sum_{i=1}^{n-1} w'_i$ and $u' = (u_1, ..., u_{n-1})$. Thus,

$$f_\chi(u) = 2^{-n} \sum_{w' \in GF(2)^{n-1}} \widehat{f_\chi}(w', h(w'))(-1)^{w' \cdot (u' + u_n(1, ..., 1))}$$

and, therefore, $f(u) = g(u' + u_n(1, ..., 1))$, where $g(u') = f(u', 0)$ is perfect nonlinear. We obtain a function of the form (1).

Clearly, only the functions of the form (1) satisfy $PC(n-1)$. This case had already been studied by Preneel *et al.*, in [25]. ∎

*Remark.* We do not know how to characterize those functions satisfying $PC(n-3)$. Proposition 1 leads then to sums over three-dimensional flats, and it seems hard to generalize Lemma 3 to sums of eight squares.

## 4. FUNCTIONS SATISFYING $PC(\ell)$ OF HIGH ORDER

### 4.1. Functions Satisfying $PC(\ell)$ of Order $n-\ell$

A function $f$ satisfies $PC(\ell)$ of order $k = n-\ell$ if and only if every restriction of $f$ obtained by keeping constant $n-\ell$ coordinates is perfect nonlinear. Thus, $\ell$ must be even.

For $n$ even, these functions were characterized in [8]. They were called *hyper-bent*.

We give this characterization in Proposition 7 for $n$ even and extend it to $n$ odd. This generalizes the particular case $\ell = 1$ that has already been studied by Preneel *et al.*, in [25]. We give also a simplified proof of this characterization.

PROPOSITION 7. *For every $n \geqslant 4$ and every even $\ell$ such that $2 \leqslant \ell \leqslant n-2$, the functions $f$ which satisfy $PC(\ell)$ of order $n-\ell$ are the functions of the form*

$$f(x_1, ..., x_n) = \sum_{1 \leqslant i < j \leqslant n} x_i x_j + h(x_1, ..., x_n), \tag{5}$$

*where $h$ is affine. For every odd $n \geqslant 3$, the functions $f$ which satisfy $PC(n-1)$ of order 1 are the functions of the form (1) (cf. the statement of Proposition 6).*

*Proof.* Assume first that $n \geqslant 4$ is even and $\ell = 2$. Since the only perfect nonlinear functions on $GF(2)^2$ are the functions $x_1 x_2 + h(x_1, x_2)$, where $h$ is affine, the functions satisfying $PC(2)$ of order $n-2$ must have the form (5). The converse is also straightforward.

Consider now the more general case: $n \geqslant 4$ even, $\ell$ even, and $2 \leqslant \ell \leqslant n-2$. Any function $f$ of the form (5) is perfect nonlinear; it is a simple matter to check that its associated symplectic form is nondegenerate. Consequently, $f$ satisfies $PC(\ell)$ of order $n-\ell$ for every even $\ell$, since any of its restrictions obtained by keeping constant $n-\ell$ coordinates of $x$ has the same form as $f$ itself. Conversely, let $f$ satisfy $PC(\ell)$ of order $n-\ell$. Consider any of its restrictions $f'$ obtained by keeping constant $n-\ell-2$ coordinates of $x$. The function $f'$ is a Boolean function on $GF(2)^{\ell+2}$ and satisfies $PC(\ell)$ of order 2. According to Proposition 6 and since it satisfies $PC(\ell)$, it is perfect nonlinear; i.e., it satisfies $PC(\ell+2)$. We deduce that $f$ satisfies $PC(\ell+2)$ of order $n-\ell-2$. By induction, we deduce that $f$ satisfies $PC(n-2)$ of order 2 and $PC(n)$ as well. According to Proposition 5, its dual $\tilde{f}$ satisfies $PC(2)$ of order $n-2$, i.e., it has the form (5). It is now a simple matter to check that $f$ has then the same form: $\tilde{f}$ satisfies $PC(n-2)$ of order 2; according to Proposition 5 once again, $f$ satisfies $PC(2)$ of order $n-2$; i.e., it has the form (5).

We treat now the case $n$ odd. Assume first that $\ell \leqslant n-2$. Any function of the form (5) clearly satisfies $PC(\ell)$ of order $n-\ell$. Conversely, let $f$ satisfy $PC(\ell)$ of order $n-\ell$. Since $n-1$ is even and $\ell \leqslant n-3$, any restriction of $f$ obtained by keeping one coordinate constant is equal to $\sum_{1 \leqslant i < j \leqslant n-1} x_i x_j + h(x_1, ..., x_{n-1})$, where $h$ is affine. It is a simple matter to deduce that $f$ has the form (5). Assume now that $\ell = n-1$. According to Proposition 6, any function $f$ satisfying $PC(n-1)$ of order 1 has the form

$$f(x_1, ..., x_n) = g(x_1 + x_n, ..., x_{n-1} + x_n) + h(x)$$

where $g$ is perfect nonlinear and $h$ is affine, since it satisfies $PC(n-1)$; the converse is also clear. ∎

### 4.2. Functions Satisfying $PC(\ell)$ of Order $n-\ell-1$

PROPOSITION 8. *For every positive even $\ell$ and every $n \geqslant \ell+1$, the functions $f$ satisfying $PC(\ell)$ of order $n-\ell-1$ are the same as those which satisfy $PC(\ell)$ of order $n-\ell$. For every odd $\ell \geqslant 3$ and every $n \geqslant \ell+1$, the functions $f$ satisfying $PC(\ell)$ of order $n-\ell-1$ are the same as those which satisfy $PC(\ell+1)$ of order $n-\ell-1$.*

*Proof.* Let $f$ satisfy $PC(\ell)$ of order $n-\ell-1$. We assume first that $\ell$ is even.

If $\ell \leqslant n-2$, then every restriction of $f$ obtained by keeping constant $n-\ell-2$ coordinates is a Boolean function on $GF(2)^{\ell+2}$ and satisfies $PC(\ell)$, since it satisfies $PC(\ell)$ of order 1. Thus, it satisfies $PC(\ell+2)$, according to Proposition 6 (applied

with $\ell+2$ in the place of $n$). Hence, $f$ satisfies $PC(\ell+2)$ of order $n-\ell-2$, and has the form (5), according to Proposition 7. Therefore, it satisfies $PC(\ell)$ of order $n-\ell$. The converse is obvious.

For $\ell=n-1$ ($n$ odd), we have seen in Proposition 7 that the functions which satisfy $PC(n-1)$ are the same as those which satisfy $PC(n-1)$ of order 1.

We assume now that $\ell$ is odd. Every restriction of $f$ obtained by keeping constant $n-\ell-1$ coordinates is a Boolean function on $GF(2)^{\ell+1}$ and satisfies $PC(\ell)$. Thus, according to Proposition 6 (applied with $\ell+1$ in the place of $n$), it satisfies $PC(\ell+1)$. Thus, $f$ satisfies $PC(\ell+1)$ of order $n-\ell-1$. The converse is obvious. ▮

### 4.3. *Functions Satisfying $PC(\ell)$ of Order $n-\ell-2$*

The determination of these functions is more difficult. The key-result is the following.

PROPOSITION 9. *For every even $n\geqslant 8$, the functions $f$ satisfying $PC(n-3)$ of order* 1 *are the functions of the form* (5).

*Proof.* Clearly, every function of the form (5) satisfies $PC(n-3)$ of order 1.

Conversely, we shall first prove that any function $f$ satisfying $PC(n-3)$ of order 1 is perfect nonlinear. Suppose the contrary; then $f$ does not satisfy $PC(n-2)$, according to Proposition 6. We shall prove that this leads to a contradiction. Function $f$ satisfies $PC(n-3)$, according to Proposition 2, and does not satisfy $PC(n-2)$. Thus, there exists a word $a\in GF(2)^n$ of weight $n-2$, such that the function $f(x)+f(x+a)$ is not balanced. We can, without loss of generality assume that $a=(0, 0, 1, ..., 1)$. Set $a'=(0, 1, ..., 1)\in GF(2)^{n-1}$. Let $f_0$ (resp. $f_1$, $f'_0$, $f'_1$) be the restrictions of $f$ obtained by keeping $x_1$ equal to 0 (resp. $x_1$ equal to 1, $x_2$ equal to 0, $x_2$ equal to 1). The functions $f_0$, $f_1$, $f'_0$, and $f'_1$ are Boolean functions on $GF(2)^{n-1}$ and satisfy $PC(n-3)$, by hypothesis. Thus, according to Proposition 6, any of the functions $f_0(x)+f_0(x+a')$, $f_1(x)+f_1(x+a')$, $f'_0(x)+f'_0(x+a')$, and $f'_1(x)+f'_1(x+a')$ is either constant or balanced.

Since the function $f(x)+f(x+a)$ is not balanced, one of the functions $f_0(x)+f_0(x+a')$, $f_1(x)+f_1(x+a')$, and one of the functions $f'_0(x)+f'_0(x+a')$, $f'_1(x)+f'_1(x+a')$ must be constant. We can without loss of generality assume that these constant functions are $f_0(x)+f_0(x+a')$ and $f'_0(x)+f'_0(x+a')$ (otherwise, if for instance they are $f_1(x)+f_1(x+a')$ and $f'_0(x)+f'_0(x+a')$, we can change $f(x_1, ..., x_n)$ into $f(x_1+1, x_2, ..., x_n)$). We can also assume that their constant value is 0 (otherwise, they are both equal to 1, since, being constant, they must be equal one to each other, and we can change $f$ into $f+1$).

Let $f''_{0,0}$ (resp. $f''_{0,1}, f''_{1,0}, f''_{1,1}$) be the restrictions of $f$ obtained by keeping $(x_1, x_2)$ equal to $(0, 0)$ (resp. $(0, 1)$, $(1, 0)$, $(1, 1)$). Set $a''=(1, ..., 1)\in GF(2)^{n-2}$. We have $f''_{0,0}(x)+f''_{0,0}(x+a'')=f''_{0,1}(x)+f''_{0,1}(x+a'')=f''_{1,0}(x)+f''_{1,0}(x+a'')=0$. Since the functions $f_1(x)+f_1(x+a')$ and $f'_1(x)+f'_1(x+a')$ are either constant or balanced, $f''_{1,1}(x)+f''_{1,1}(x+a'')$ must be either equal to the constant function 0 or to the constant function 1. Say $f''_{1,1}(x)+f''_{1,1}(x+a'')=\varepsilon$, $\varepsilon\in GF(2)$. From the equalities

$f''_{0,0}(x)+f''_{0,0}(x+a'')=f''_{0,1}(x)+f''_{0,1}(x+a'')=f''_{1,0}(x)+f''_{1,0}(x+a'')=0$ and $f_{1,1}(x)+f''_{1,1}(x+a'')=\varepsilon$, we deduce

$$f(x+a)=f(x)+\varepsilon\, x_1x_2.$$

Let $g$ be the restriction of $f$ to the hyperplane of equation $x_n=0$. We have, for every $(x_1, ..., x_{n-1})\in GF(2)^{n-1}$:

$$f(x_1, ..., x_{n-1}, 1)=g(x_1, x_2, x_3+1, ..., x_{n-1}+1)+\varepsilon\, x_1x_2.$$

We deduce

$$f(x_1, ..., x_n)=g(x_1, x_2, x_3+x_n, ..., x_{n-1}+x_n)+\varepsilon\, x_1x_2x_n.$$

We show now that the case $\varepsilon=0$ is impossible. In this case, we have, for any word $u=(u_1, ..., u_n)$:

$$\begin{aligned}f(x_1, ..., x_n)+f(x_1+u_1, ..., x_n+u_n)\\ =g(x_1, x_2, x_3+x_n, ..., x_{n-1}+x_n)\\ +g(x_1+u_1, x_2+u_2, x_3+x_n+u_3+u_n, ..., x_{n-1}+x_n+u_{n-1}+u_n).\end{aligned}$$

Since $f$ satisfies $PC(n-3)$, for every nonzero word $u$ of weight smaller than or equal to $n-3$, the function on $GF(2)^{n-1}$,

$$g(x_1, x_2, x_3, ..., x_{n-1})+g(x_1+u_1, x_2+u_2, x_3+u_3+u_n, ..., x_{n-1}+u_{n-1}+u_n),$$

is balanced (its weight is half the weight of the function $f(x_1, ..., x_n)+f(x_1+u_1, ..., x_n+u_n)$ which is balanced). But, when $u$ ranges over the set of all those nonzero words of length $n$ whose weights are smaller than or equal to $n-3$, the word $(u_1, u_2, u_3+u_n, ..., u_{n-1}+u_n)$ ranges over the set of all the nonzero words of length $n-1$. Taking $u_n=0$, we obtain all the nonzero words of weights smaller than or equal to $n-3$; taking $u_n=1$, we obtain, among others, all the words of weights greater than or equal to $n-2$ (any such word $v$ is obtained from the word $u=(v_1, v_2, v_3+1, ..., v_{n-1}+1, 1)$ which has weight smaller than or equal to $4\leqslant n-3$). Thus, $g$ is perfect nonlinear, which is impossible since $n-1$ is odd.

We show finally that the case $\varepsilon=1$ is also impossible. By hypothesis, the restrictions of $f$ to the hyperplanes of equations $x_n=0$ and $x_3=0$ both satisfy $PC(n-3)$. The first one is $g$ and the second one is the function

$$f(x_1, x_2, 0, x_4, ..., x_n)=g(x_1, x_2, x_n, x_4+x_n, ..., x_{n-1}+x_n)+x_1x_2x_n.$$

We deduce that $g$ and the function

$$r(x_1, x_2, ..., x_{n-1})=g(x_1, x_2, x_3, x_4+x_3, ..., x_{n-1}+x_3)+x_1x_2x_3$$

both satisfy $PC(n-3)$. According to Proposition 6, $g$ admits one linear structure $b$ of weight greater than or equal to $n-2$. Set $c=(b_1, b_2, b_3, b_4+b_3, ..., b_{n-1}+b_3)$. We have, for every $x \in GF(2)^{n-1}$:

$$\begin{aligned} r(x)+r(x+c) = {} & g(x_1, x_2, x_3, x_4+x_3, ..., x_{n-1}+x_3) \\ & + g(x_1+b_1, x_2+b_2, x_3+b_3, x_4+x_3+b_4, ..., x_{n-1}+x_3+b_{n-1}) \\ & + x_1x_2x_3 + (x_1+b_1)(x_2+b_2)(x_3+b_3). \end{aligned}$$

Since, $b$ is a linear structure of $g$, the function $g(x_1, x_2, x_3, x_4+x_3, ..., x_{n-1}+x_3)+g(x_1+b_1, x_2+b_2, x_3+b_3, x_4+x_3+b_4, ..., x_{n-1}+x_3+b_{n-1})$ is constant. The functions $x_1x_2x_3$ and $(x_1+b_1)(x_2+b_2)(x_3+b_3)$ having both weight $2^{n-4}$ and being different one from each other (since $b$ has weight greater than or equal to $n-2$), the function $r(x)+r(x+c)$ cannot be constant nor balanced. A contradiction with Proposition 6.

Hence, $f$ is perfect nonlinear. According to Proposition 5, its dual $\tilde{f}$ satisfies the criterion $SAC(n-3)$. Thus, according to the bound on the degree of the functions satisfying $SAC(k)$ recalled in the Introduction, it has degree smaller than or equal to 2. Since every restriction of $\tilde{f}$ obtained by keeping constant $n-3$ coordinates of $x$ satisfies $SAC$ and therefore has at least two terms of degree 2 in its algebraic normal form, the algebraic normal form of $\tilde{f}$ must be equal to $\sum_{\{i,j\} \in I} x_i x_j + h(x)$, where $h$ is affine and where $I$ is such that for any $i$ there exists at most one index $j$ such that $\{i, j\} \notin I$. We deduce that $\tilde{f}$ has the form (5). Suppose that, for instance, the term $x_1 x_2$ is missing in the algebraic normal form of $\tilde{f}$; then, because of the property of $I$, we would have

$$\tilde{f}(x) = (x_1+x_2)\left(\sum_{i=3}^{n} x_n\right) + g(x_3, ..., x_n)$$

and such a function cannot be perfect nonlinear, since it is linearly equivalent to a function independent of $x_1$. The function $\tilde{f}$ has the form (5); $f$ has the same form, as shown already in the proof of Proposition 7. ∎

*Remark.* In Proposition 9, the condition $n \geqslant 8$ cannot be weakened. For $n \leqslant 6$, the functions satisfying $PC(n-3)$ of order 1 are not necessarily perfect nonlinear. For instance, let $r$ be a perfect nonlinear function on $GF(2)^4$ and let $f$ be the function on $GF(2)^6$ defined by:

$$f(x_1, ..., x_6) = r(x_1+x_5+x_6, x_2+x_5+x_6, x_3+x_5, x_4+x_6).$$

$f$ is not perfect nonlinear since it admits the linear structure $(0, 0, 1, 1, 1, 1)$. It satisfies $PC(n-3)$ of order 1, since all of its restrictions obtained by keeping constant one coordinate satisfy $PC(3)$. For instance, keep constant $x_1=0$; then the function $f(0, x_1, ..., x_5) = r(x_4+x_5, x_1+x_4+x_5, x_2+x_4, x_3+x_5)$ has the form (2) with $g(x_1, ..., x_4) = r(x_4, x_1+x_4, x_2+x_4, x_3)$ (which is a perfect nonlinear function since $r$ is one), $h(x)=0$, and $i=3$.

THEOREM 1. *For every positive even $\ell \leqslant n-4$ (with $n \geqslant 6$) and every odd $\ell$ such that $5 \leqslant \ell \leqslant n-5$ (with $n \geqslant 10$), the functions which satisfy $PC(\ell)$ of order $n-\ell-2$ are functions of the form*

$$\sum_{1 \leqslant i < j \leqslant n} x_i x_j + h(x_1, ..., x_n),$$

*where $h$ is affine.*

*Proof.* We already have seen that the functions of the form (5) satisfy $PC(\ell)$ of order $n-\ell-2$. Conversely, assume that $\ell$ is even, $\ell \leqslant n-4$. Every restriction of $f$ obtained by keeping constant $n-\ell-2$ coordinates satisfies $PC(\ell+2)$, according to Proposition 6 (it satisfies $PC(\ell)$ and we have $\ell+2 \geqslant 4$). Thus $f$ satisfies $PC(\ell+2)$ of order $n-\ell-2$ and has form (5).

Assume that $\ell$ is odd. Any restriction of $f$ obtained by keeping constant $n-\ell-3$ coordinates is a Boolean function on $GF(2)^{\ell+3}$ and satisfies $PC(\ell)$ of order 1. According to Proposition 9 and since $\ell+3 \geqslant 8$, it has the form (5). Thus, $f$ has the form (5) as well. ▮

COROLLARY 1. *Under the hypothesis of Theorem* 1, *there does not exist any function satisfying $EPC(\ell)$ of order $k \geqslant n-\ell-2$.*

*Proof.* Let us check that any function of the form (5) cannot satisfy $EPC(\ell)$ of order $k$. Let $a$ be any nonzero word. The function $f(x)+f(x+a)$ is equal to:

$$\sum_{1 \leqslant i \neq j \leqslant n} a_i x_j + \eta, \qquad \eta \in GF(2).$$

Let $\omega$ be the Hamming weight of the word whose $j$th coordinate is equal to the coefficient of $x_j$ in this algebraic normal form, that is, $\sum_{i \neq j} a_i$. The function $f(x)+f(x+a)$ is $(\omega-1)$-resilient and it is not $\omega$-resilient (cf. [6]). Choose $a$ of weight 2; then $\omega = 2$. We deduce that $f$ does not satisfy $EPC(\ell)$ of order $k$, since $k \geqslant 2$. ▮

*Open question.* What is the maximum value of $k$ for which there exist Boolean functions on $GF(2)^n$ satisfying $EPC(\ell)$ of order $k$?

## 5. CONSTRUCTION OF NONQUADRATIC FUNCTIONS SATISFYING *EPC*($\ell$) OF ORDER $k$

We have seen above that, for $n$ sufficiently large:

— the functions satisfying $PC(\ell)$ of order $k \geqslant n-\ell-2$ are all quadratic (i.e., have algebraic degree 2, which is a cryptographic drawback; cryptosystems using such functions do not resist some known attacks; cf. [21] for instance);

— there is no function satisfying $EPC(\ell)$ of order $k \geqslant n-\ell-2$.

We want now to design nonquadratic functions satisfying $EPC(\ell)$ of order $k$.

### 5.1. The Maiorana–McFarland Construction

A construction of functions satisfying $PC(\ell)$ of order $k$ which uses a general method for designing Boolean cryptographic functions is given in [23]. This method was first introduced by Maiorana and McFarland in the 1970s to design bent functions (cf. [16]).

DEFINITION 2. We call the *Maiorana–McFarland* function any Boolean function $f$ defined as on $GF(2)^n$

$$f(x, y) = x \cdot \phi(y) + g(y), \qquad x \in GF(2)^s, \quad y \in GF(2)^t, \tag{6}$$

where "$\cdot$" is the usual inner product in $GF(2)^s$, $s, t$ are any positive integers; $n = s + t$; $g$ is any Boolean function on $GF(2)^t$, and $\phi$ is any mapping from $GF(2)^t$ to $GF(2)^s$.

This construction has been used in [6, 9] to design resilient functions. Kurosawa and Satoh use it in [23] to obtain nonquadratic $PC(\ell)$ of order $k$ functions. The mappings $\phi$ considered by these authors are linear. We believe this is a weakness: the nonquadraticity of their function $f$ comes from the fact that the function $g$ involved in its definition is nonquadratic. But the fact that $f$ satisfies $PC(\ell)$ of order $k$ is independent of the choice of $g$. Thus, it must be possible to find an attack on a cryptosystem using such a function, by using this peculiarity.

We study now the Maiorana–McFarland functions $f(x, y) = x \cdot \phi(y) + g(y)$ in the general case, i.e., where $\phi$ is not necessarily linear. We show that we can, in this wider framework, obtain functions which satisfy $EPC(\ell)$ of order $k$, thanks to a deep result on the dual distance of nonlinear codes, due to Delsarte. Notice that the nonquadraticity of these functions is independent of the choice of $g$. We check that $g$ can be chosen so that $f$ is also resilient, with high nonlinearity.

### 5.2. Preliminaries on Resilient Functions

We shall use in the sequel the following well-known properties:

*Property* 1. if $f$ is $k$-resilient from $GF(2)^n$ to $GF(2)^m$ and if $g$ is balanced on $GF(2)^m$, then $g \circ f$ is $k$-resilient;

*Property* 2. if $C$ is a linear $[n, k, d]$ code (i.e., a linear code of length $n$, dimension $k$ and minimum distance $d$) and if $G$ is a generator matrix of $C$, then the function $x \in GF(2)^n \to x \times G^t$, where $G^t$ is the transposed matrix of $G$, is $(d-1)$-resilient.

Property 1 is straightforward. Property 2, that will be generalized by Corollary 3, is a consequence of the fact that if $k \leqslant n$ and if $M$ is a $k \times n$ matrix of rank $k$ then the function $x \to xM^t$ is balanced. Since $C$ has minimum weight $d$, it is not possible by deleting at most $d-1$ columns of $G$ to obtain a matrix of rank smaller than $k$.

We shall use also a result from Delsarte [13].

LEMMA 4 [13]. *A Boolean function $f$ on $GF(2)^n$ is $k$th order correlation-immune if and only if, for every nonzero $b \in GF(2)^n$ of weight smaller than or equal to $k$, the restriction of the linear form $x \to b \cdot x$ (where "$\cdot$" is the usual inner product on $GF(2)^n$) to the support of $f$ (i.e., the set $\{x \in GF(2)^n \mid f(x) = 1\}$) is balanced.*

The resilience order of the Maiorana–McFarland functions has been determined in [6].

PROPOSITION 10. *Let $f$ be a Maiorana–McFarland function of the form (6). If every word of the set $\phi(GF(2)^t)$ has weight greater than or equal to $k+1$, then $f$ is $k$-resilient.*

### 5.3. Maiorana–McFarland Functions Satisfying EPC($\ell$) of Order $k$

PROPOSITION 11. *Any Maiorana–McFarland function,*

$$f(x, y) = x \cdot \phi(y) + g(y),$$

*with $\phi = (\phi_1, ..., \phi_s)$, satisfies the criterion EPC($\ell$) of order $k$ if and only if*:

1. *the sum of at least 1 and at most $\ell$ coordinates $\phi_i$ of $\phi$ is $k$-resilient*;
2. *if $y$ and $z$ are two different elements of $GF(2)^t$, at Hamming distance smaller than or equal to $\ell$ to each other, the Hamming distance between $\phi(y)$ and $\phi(z)$ is greater than or equal to $k+1$.*

*Proof.* For every $a \in GF(2)^s$ and every $b \in GF(2)^t$, we have

$$f(x, y) + f(x+a, y+b) = x \cdot [\phi(y) + \phi(y+b)] + a \cdot \phi(y+b) + g(y) + g(y+b).$$

Assume that conditions 1 and 2 are satisfied. If $b = 0$ and $1 \leqslant w(a) \leqslant \ell$, then because of condition 1, the function $f(x, y) + f(x+a, y) = a \cdot \phi(y)$ is $k$-resilient. If $1 \leqslant w(b) \leqslant \ell$, then the function $f(x, y) + f(x+a, y+b)$ is a Maiorana–McFarland function and is $k$-resilient, thanks to condition 2 and to Proposition 10. The converse is similar. ∎

We consider now mappings of the form $\phi_2 \circ \phi_1$, where $\phi_1$ is a mapping from $GF(2)^t$ to $GF(2)^r$ and $\phi_2$ is a mapping from $GF(2)^r$ to $GF(2)^s$. This allows us to split the conditions of Proposition 11 into several simpler ones.

PROPOSITION 12. *A sufficient condition for a mapping of the form $\phi_2 \circ \phi_1$ to satisfy conditions 1 and 2 of Proposition 7 is that*:

1. (a) *The mapping $\phi_1$ is $k$-resilient*;

   (b) *if two different words $y$ and $z$ are at distance smaller than or equal to $\ell$, one to each other, then $\phi_1(y) \neq \phi_1(z)$.*

2. (a) *The sum of at least one and at most $\ell$ coordinates of $\phi_2$ is balanced*;

   (b) *if $y \neq z$, then $\phi_2(y)$ and $\phi_2(z)$ are at distance greater than or equal to $k+1$, one to each other.*

*Proof.* Condition 1 of Proposition 11 is satisfied thanks to conditions 1a and 2a (according to property 1). Condition 2 is clearly satisfied thanks to the two others. ▮

The construction given by Kurosawa and Satoh in [23] respects the conditions of Proposition 12. The mappings $\phi_1$ and $\phi_2$ are linear; $\phi_1(x) = x\,G_1^t$ and $\phi_2(x) = x\,G_2$, where $G_1$ and $G_2$ are the generator matrices of two linear codes $C_1$ and $C_2$. The conditions are then fulfilled by the facts that the codes $C_1$ and $C_2$ are assumed to have minimum distances greater than or equal to $k+1$ and dual distances (i.e., minimum distances of their duals) greater than or equal to $\ell+1$:

— $C_1$ having minimum distance greater than or equal to $k+1$, condition 1a is fulfilled, according to property 2.

— $C_1^\perp$ having minimum distance greater than or equal to $\ell+1$, condition 1b is fulfilled, since $\phi_1$ is the syndrome function of $C_1^\perp$ (cf. [29] for a definition of the syndrome);

— $C_2^\perp$ having minimum distance greater than or equal to $\ell+1$, the sum of at least one and at most $\ell$ columns of its parity check matrix $G_2$ is nonzero (cf. [29]); the $i$th coordinate of $\phi_2(x)$ is equal to the dot product between $x$ and the $i$th column of $G_2$. Thus, the sum of at least one and at most $\ell$ coordinates of $\phi_2$ is a nonzero linear form; it is therefore balanced and condition 2a is fulfilled;

— $C_2$ having minimum distance greater than or equal to $k+1$, condition 2b is fulfilled, by definition.

### *5.4. Using Nonlinear Codes*

We want now to design nonlinear mappings $\phi_1$ and $\phi_2$ satisfying the conditions of Proposition 12. The keynotion will be that of dual distance of a (nonlinear) code.

DEFINITION 3. Let $C$ be a (nonlinear) code of length $n$ (i.e., a subset of $GF(2)^n$). The distance enumerator of $C$ is the polynomial in two variables:

$$D_C(X, Y) = \frac{1}{|C|} \sum_{x,\, y \in C} X^{n-d(x,\, y)} Y^{d(x,\, y)}$$

where $d(x, y)$ is the Hamming distance between the words $x$ and $y$. The dual distance of $C$ is the smallest positive integer $i$ such that the coefficient of the monomial $X^{n-i}Y^i$ in the polynomial $D_C(X+Y, X-Y)$ is nonzero.

When the code is linear, the dual distance is equal to the minimum distance of the dual code, thanks to MacWilliams identity (cf. [29]). Even when the code is not necessarily linear, the dual distance plays an important role, thanks to a result due to Delsarte [14], which can be stated as follows.

PROPOSITION 13. *Let $C$ be a code of dual distance $d^\perp$. The indicator of $C$ (i.e., the Boolean function whose support is $C$) is a $(d^\perp-1)$th order correlation immune function.*

We deduce the following two corollaries.

COROLLARY 2. *Let $C$ be a code of length $n$ and dual distance $d^\perp$. Then, for every set $I \subset \{1, ..., n\}$ such that $1 \leqslant |I| \leqslant d^\perp - 1$, the function $\sum_{i \in I} x_i$ is balanced on $C$.*

This is a direct consequence of Proposition 13 and Lemma 4.

COROLLARY 3. *Let $\phi$ be a mapping from $GF(2)^t$ to $GF(2)^r$. If all the codes $\phi^{-1}(c)$; $c \in GF(2)^r$, have the same cardinality and dual distances greater than or equal to $k+1$, then $\phi$ is $k$-resilient.*

This is a consequence of Proposition 13 and of the obvious fact that $\phi$ is $k$-resilient if and only if all the sets $\phi^{-1}(c)$, $c \in GF(2)^r$, have the same cardinality and if, for any $c$ in $GF(2)^r$, the indicator of $\phi^{-1}(c)$ (i.e., the Boolean function whose support is $\phi^{-1}(c)$) is a $k$th order correlation-immune function.

From Proposition 12 and Corollaries 2 and 3, we deduce

PROPOSITION 14. *Let $\phi$ be a mapping of the form $\phi = \phi_2 \circ \phi_1$*; assume that:

1. (a) *the codes $\phi_1^{-1}(c)$, $c \in GF(2)^r$, have the same cardinality and dual distances greater than or equal to $k+1$;*

   (b) *these same codes have minimum distances greater than or equal to $\ell+1$;*

2. *$\phi_2$ is injective and*

   (a) *the code $\phi_2(GF(2)^r)$ has dual distance greater than or equal to $\ell+1$;*

   (b) *this same code has minimum distance greater than or equal to $k+1$.*

*Then, $\phi$ fulfils the conditions of Proposition* 11.

*Proof.* Condition 1a of Proposition 14 implies condition 1a of Proposition 12, thanks to Corollary 3. Conditions 1b and 2b of Proposition 14 clearly imply conditions 1b and 2b of Proposition 12. Condition 2a of Proposition 14 implies condition 2a of Proposition 12, thanks to Corollary 2. Thus, the hypotheses of Proposition 12 are satisfied, which implies that the conditions of Proposition 11 are satisfied. ▮

We carry on the simplification of the conditions by considering systematic codes (cf. [29]; see also [31]).

DEFINITION 4. A binary code $C$ of length $n$ is called systematic if there exists a subset $I$ of $\{1, ..., n\}$ called an *information set* of $C$, such that every possible tuple occurs in exactly one codeword within the specified coordinates $x_i$, $i \in I$.

Denoting by $E_I$ the vector-space $\{e \in GF(2)^n \mid \forall i \in I,\ e_i = 0\}$, the set of all the cosets $C+e$, $e \in E_I$ is then a partition of $GF(2)^n$.

Let $\phi_1$ be the mapping $x \to e \in E_I \mid x \in C+e$. Then all the codes $\phi_1^{-1}(e) = C+e$; $e \in E_I$ have the same cardinality, the same distance enumerator and, therefore, the same minimum distance and the same dual distance.

THEOREM 2. *Let $C_1$ be a systematic code of length $t$ and information set $I = \{r+1, ..., t\}$. Let $\phi_1$ be the mapping*

$$y \in GF(2)^t \to e \in GF(2)^r \mid y \in C_1 + (e_1, ..., e_r, 0, ..., 0),$$

*or more generally any mapping from $GF(2)^t$ to $GF(2)^r$ such that the reverse image of every element of $GF(2)^r$ is a coset of $C_1$. Let $\phi_2$ be an injective mapping from $GF(2)^r$ to $GF(2)^s$ $(s > r)$ and $C_2$ the code equal to $\phi_2(GF(2)^r)$. Assume that*

1. *$C_1$ has minimum distance greater than or equal to $\ell+1$ and dual distance greater than or equal to $k+1$;*

2. *$C_2$ has dual distance greater than or equal to $\ell+1$ and minimum distance greater than or equal to $k+1$;*

*then, for every Boolean function $g$ on $GF(2)^t$, the function $f(x, y) = x \cdot (\phi_2 \circ \phi_1)(y) + g(y)$, $x \in GF(2)^s$, $y \in GF(2)^t$, where "$\cdot$" denotes the usual inner product in $GF(2)^s$, satisfies EPC($\ell$) of order $k$.*

Every linear code is systematic (cf. [29]). Thus, this result includes that of Kurosawa and Satoh [23] as a particular case.

*Remark.* The mapping $\phi_1$ (resp. $\phi_2$) above can be composed (on the left) with any permutation on $GF(2)^r$ (resp. on $C_2$). Thus, the function $x \cdot (\phi_2 \circ \phi_1)(y)$ above can have high degree, even if $C_1$ and $C_2$ are linear.

### *5.5 The Deduced Nonquadratic Functions*

There exist several known (infinite classes of) nonlinear systematic codes. The two most famous are the $(2^m, 2^{2m}, 2^{m-1} - 2^{m/2-1})$ Kerdock code $\mathscr{K}_m$ ($m$ even $\geqslant 4$; we give here the length, the cardinality, and the minimum distance) whose dual distance is 6 and the $(2^m, 2^{2^m - 2m}, 6)$ Preparata code $\mathscr{P}_m$, whose dual distance is $2^{m-1} - 2^{m/2-1}$.

All of these codes happen to have strictly better parameters than linear codes; for instance, it is proved in [3] that the Preparata code has at least twice as many codewords as any linear code with the same length and minimum distance and that the Kerdock code has more codewords than any linear code with the same length and dual distance.

5.1.1. *Explicit Examples of such functions.* Let us apply Theorem 2 with $C_1$ equal to the Preparata code and $C_2$ equal to the Kerdock code (resp. with $C_2$ equal to the Preparata code and $C_1$ equal to the Kerdock code), we deduce

COROLLARY 4. *For any even $m \geqslant 4$, there exists a mapping $\phi: GF(2)^{2^m} \to GF(2)^{2^m}$ such that, for any Boolean function $g$ on $GF(2)^{2^m}$, the function $f(x, y) = x \cdot \phi(y) + g(y)$ is a nonquadratic Boolean function on $GF(2)^{2^{m+1}}$ satisfying EPC(5) of order $2^{m-1} - 2^{m/2-1} - 1$ (resp. EPC($2^{m-1} - 2^{m/2-1} - 1$) of order 5).*

We study now the expressions of the mappings $\phi_1$ and $\phi_2$ for each of these two functions.

- We begin with the case where $C_1$ and $C_2$ are respectively equal to the Preparata code and the Kerdock code.

There exists a simple description of the Preparata code (cf. [1]): let $u = (u_\infty, u_0, ..., u_{2^{m-1}-2})$ and $v = (v_\infty, v_0, ..., v_{2^{m-1}-2})$ be two binary words of length $2^{m-1}$; let $\alpha$ be a primitive element of the finite field $GF(2^{m-1})$. The ordered pair $(u, v)$ belongs to the Preparata code if and only if the conditions are satisfied:

1. $u_\infty + \sum_{i=0}^{2^{m-1}-2} u_i = v_\infty + \sum_{i=0}^{2^{m-1}-2} v_i = 0$; i.e., $u$ and $v$ have even Hamming weights;

2. $\sum_{i=0}^{2^{m-1}-2} u_i \alpha^i = \sum_{i=0}^{2^{m-1}-2} v_i \alpha^i$;
3. $\sum_{i=0}^{2^{m-1}-2} u_i \alpha^{3i} + \sum_{i=0}^{2^{m-1}-2} v_i \alpha^{3i} = (\sum_{i=0}^{2^{m-1}-2} u_i \alpha^i)^3$.

Notice that all of these conditions are linear with respect to $v$; for this reason, it is a simple matter to exhibit an information set of $\mathscr{P}_m$. Choose a maximal set $J$ in $\{0, ..., 2^{m-1}-2\}$ such that the words $(\alpha^j, \alpha^{3j})$, $j \in J$, are linearly independent over $GF(2)$. The cardinality of $J$ is equal to $2m-2$ (cf. [1], for instance). Then, taking all of the indices $0, ..., 2^{m-1}-2$ of $u$ on one hand, and those of $v$ which do not belong to $J$ on the other hand, we obtain an information set of $\mathscr{P}_m$, since the other coordinates of the words $u$ and $v$ are uniquely determined by the linear nondegenerate system given by relations 1, 2, and 3.

This leads to the mapping $\phi_1 : GF(2)^{2^m} \to GF(2)^{2m}$ satisfying the hypothesis of Theorem 2. Denote by $(\eta, \tau, \beta, \gamma)$ the word of $GF(2)^2 \times GF(2^{m-1})^2$ defined by

$$\begin{aligned}
\eta &= u_\infty + \sum_{i=0}^{2^{m-1}-2} u_i, \\
\tau &= v_\infty + \sum_{i=0}^{2^{m-1}-2} v_i, \\
\beta &= \sum_{i=0}^{2^{m-1}-2} \alpha^i (u_i + v_i), \\
\gamma &= \sum_{i=0}^{2^{m-1}-2} \alpha^{3i}(u_i + v_i) + \left( \sum_{i=0}^{2^{m-1}-2} \alpha^i u_i \right)^3.
\end{aligned} \tag{7}$$

As defined in Theorem 2, $\phi_1(u, v)$ is the word of length $2m$ whose $2m-2$ last coordinates are the solutions of the system

$$\sum_{j \in J} w_j \alpha^j = \beta$$

$$\sum_{j \in J} w_j \alpha^{3j} = \gamma$$

and whose two first ones are equal to $\eta$ and to $\tau + \sum_{j \in J} w_j$. Thus, $\phi_1(u, v)$ is the composition of the mapping $(u, v) \to (\eta, \tau, \beta, \gamma)$ with a (linear) bijection from $GF(2)^2 \times GF(2^{m-1})^2$ to $GF(2)^{2m}$. This means that we can take more simply:

$$\phi_1(u, v) = (\eta, \tau, \beta, \gamma).$$

Let us recall now the definition of the Kerdock code. Write $m = 2t+2$; define for every $\gamma \in GF(2^{m-1})$ the function on $GF(2^{m-1}) \times GF(2)$,

$$f_\gamma(x, \varepsilon) = \mathrm{tr}\left( \sum_{i=1}^{t} (\gamma x)^{2^i+1} \right) + \varepsilon \, \mathrm{tr}(\gamma x), \tag{8}$$

where tr denotes the trace function from $GF(2^{m-1})$ to $GF(2)$. If we identify any Boolean function with the word equal to its list of values, the Kerdock code is the

set of Boolean functions belonging to the cosets $f_\gamma + R(1, m)$ of the Reed–Muller code $R(1, m)$.

We can take for $\phi_2$ the function defined on $GF(2)^2 \times (GF(2^{m-1}))^2$ whose value at $(\eta, \tau, \beta, \gamma)$ is the (list of values of the) function

$$f_\gamma(x, \varepsilon) + \mathrm{tr}(\beta x) + \eta\varepsilon + \tau. \tag{9}$$

The function $\gamma \mapsto f_\gamma(x, \varepsilon)$ is quadratic for every $(x, \varepsilon)$, since all the exponents $2^i + 1$ have 2-weight 2 (i.e., have a binary expansion with two 1's; cf. [29]). Thus $\phi_2$ is quadratic, and $\phi_2 \circ \phi_1$ has algebraic degree 4. But, as noticed above, we can compose $\phi_1$ and $\phi_2$ with permutations, and their degrees can be increased.

- We follow now, more briefly, with the case where $C_1$ and $C_2$ are respectively equal to the Kerdock code and the Preparata code.

We keep the same representation $(u, v)$ for the elements of the Kerdock code as for those of the Preparata code. The first half $u$ is the list of values of the restriction of the function defined in (9) which corresponds to $\varepsilon = 0$, and the second half $v$ corresponds to $\varepsilon = 1$.

Let $J$ be any subset of $\{0, ..., 2^{m-1} - 2\}$ such that $\{\alpha^j; j \in J\}$ is a basis of the $GF(2)$ vector space $GF(2)^{m-1}$. We obtain an information set of $\mathscr{K}_m$ by choosing the set of indices $\{\infty\} \cup J$ for $u$ and for $v$. Indeed, we have $\tau = u_\infty$, $\eta = \tau + v_\infty$. The relations $u_j + v_j = \mathrm{tr}(\gamma\alpha^j) + \eta$, $j \in J$, determine uniquely $\gamma$ and the relations $u_j = f_\gamma(\alpha^j, 0) + \mathrm{tr}(\beta\alpha^j) + \tau$, $j \in J$, determine then uniquely $\beta$. This permits us to determine the mapping $\phi_1$. The mapping $\phi_2$ can be easily deduced from the information set of $\mathscr{P}_m$ determined above.

*Remark.* No mapping $\phi = \phi_2 \circ \phi_1$ defined in Theorem 2 can be a permutation, since two elements in the same coset of $C_1$ have always the same image by $\phi$. Thus, function $f$ defined in this same theorem cannot be perfect nonlinear (cf. [16]). Notice, however, that the functions $f$ defined in Corollary 4 behave themselves as two dual perfect nonlinear functions satisfying the extended propagation criterion (cf. Proposition 5). It may be possible to generalize, therefore, in a manner to be defined, Proposition 5 to nonperfect nonlinear functions.

5.5.2. *Other nonlinear systematic codes with good minimum and dual distances.* The Preparata codes have been generalized into a wider class of codes with the same parameters (cf. [1]).

Another class of systematic codes with the same parameters as the Preparata codes has also been recently introduced [17]. These codes are $\mathbf{Z}_4$-linear codes, i.e., they are the images of linear codes over the ring $\mathbf{Z}_4$ of integers mod 4, by some bijection (called the Gray map) defined from $\mathbf{Z}_4$ to $GF(2)^2$ and coordinatewisely extended to the words over $\mathbf{Z}_4$. Since every linear code over $\mathbf{Z}_4$ admits, up to a permutation of the coordinates, a generator matrix of the form:

$$G = \begin{bmatrix} I_{k_1} & A & B \\ 0 & 2I_{k_2} & 2C \end{bmatrix}$$

(cf. [17]), every $\mathbf{Z}_4$-linear code is systematic.

Other examples of nonlinear systematic codes with good minimum and dual distances are the $(2^m, 2^{2m+k(m-1)}, 2^{m-1}-2^{m/2+k-1})$ Delsarte–Goethals codes ($m$ even, $k<m/2$), which are also $\mathbf{Z}_4$-linear codes and their $\mathbf{Z}_4$-duals (cf. [17]). Good candidates are also the formal duals of the Delsarte–Goethals codes studied in [15, 18] but it is not proved that all of these last codes are systematic. See also [12], where generalized Kerdock and Delsarte–Goethals codes are introduced. These codes are systematic for similar reasons as $\mathbf{Z}_4$-linear codes, but their dual distances have still to be determined.

### 5.6. *Resilience and Nonlinearity of Function f, Independently of the Choice of g*

The propagation criterion of degree $\ell$ and order $k$ is not sufficient to use a cryptographic function. The function needs also to be balanced—or, better, to be resilient of a sufficient order—and to have high nonlinearity (i.e., Hamming distance to the set of all affine functions).

According to Proposition 10, the function $f$ designed in Theorem 2 is $(w-1)$-resilient, where $w$ is the minimum weight of all the words in $C_2$ (and it is possible to check that there exist functions $g$ such that $f$ is not $w$-resilient).

Since $C_2$ can be replaced by any of its cosets (which all have the same distance enumerator), the greatest resilience order which can be achieved for such a function, independently of the choice of function $g$, is equal to the maximum distance from any word to $C_2$, i.e., the covering radius of $C_2$ (cf. [29]), minus 1.

For instance, the covering radius of the Kerdock code (resp. the Preparata code) being greater than or equal to $2^{m-1}-2^{m/2}$ (resp. being equal to 4), the function $f$ of Corollary 4 can be chosen so that it is $(2^{m-1}-2^{m/2}-1)$-resilient (resp. 3-resilient).

Let us study now the nonlinearity of $f$. The Hamming distance from a Boolean function $f$ on $GF(2)^n$ to the set of affine functions on $GF(2)^n$ is equal to

$$2^{n-1}-\tfrac{1}{2}\max_{a\in GF(2)^n}|\widehat{f_\chi}(a)|.$$

When $f$ is the Maiorana–McFarland function (6), we have

$$\begin{aligned}
&\max_{a\in GF(2)^n}|\widehat{f_\chi}(a)|\\
&\quad=\max_{a\in GF(2)^s,\, b\in GF(2)^t}\left|\sum_{x\in GF(2)^s}\left(\sum_{y\in GF(2)^t}(-1)^{x\cdot\phi(y)+g(y)+a\cdot x+b\cdot y}\right)\right|\\
&\quad=\max_{a\in GF(2)^s,\, b\in GF(2)^t}\left|\sum_{y\in GF(2)^t}\left((-1)^{g(y)+b\cdot y}\sum_{x\in GF(2)^s}(-1)^{x\cdot(a+\phi(y))}\right)\right|\\
&\quad=2^s\max_{a\in GF(2)^s,\, b\in GF(2)^t}\left|\sum_{y\in\phi^{-1}(a)}(-1)^{g(y)+b\cdot y}\right|.
\end{aligned}$$

When $f$ is defined as in Theorem 2, we obtain

$$2^{n-1} - \tfrac{1}{2} \max_{a \in GF(2)^n} |\widehat{f_\chi}(a)| = 2^{n-1} - 2^{s-1} \max_{b,\, e \in GF(2)^t} \left| \sum_{y \in e + C_1} (-1)^{g(y) + b \cdot y} \right|.$$

We deduce that, for any choice of $g$, the nonlinearity of $f$ is at least

$$2^{n-1} - 2^{s-1} |C_1|.$$

Let us consider once again the case where $C_1$ is equal to the Preparata code and $C_2$ is equal to the Kerdock code. Then, for any choice of $g$, the nonlinearity of $f$ is at least

$$2^{2^{m+1}-1} - 2^{2^{m+1}-2m-1}.$$

If $C_1$ is the Kerdock code and $C_2$ is equal to the Preparata code, then for any choice of $g$, the nonlinearity of $f$ is at least

$$2^{2^{m+1}-1} - 2^{2^m + 2m - 1}$$

which is near the (optimum) nonlinearity of perfect nonlinear functions.

*Remark.* it is possible to improve the nonlinearity of function $f$ by choosing specifically $g$ (a choice of $C_1$ being done). For instance, when $\phi$ is linear, we can choose $g$ perfect nonlinear (with $t$ even). That is what Kurosawa and Satoh do in [23]. The nonlinearity of $f$ is then greater than or equal to:

$$2^{n-1} - 2^{s + (t/2) - 1}$$

since we have, for every $a$, $b$, and $x$,

$$\left| \sum_{y \in GF(2)^t} (-1)^{x \cdot \phi(y) + g(y) + b \cdot y} \right| = 2^{t/2}.$$

This bound improves upon the bound we have obtained above when $C_1$ was equal to the Preparata code and $C_2$ was equal to the Kerdock code.

## 6. CONCLUDING REMARKS

The general construction given by Theorem 2, when applied to Kerdock and Preparata codes, leads to functions satisfying $EPC(\ell)$ of order $k$, where either $\ell$ is small and $k$ is large (in which case the function is resilient with large order and has low nonlinearity) or $\ell$ is large and $k$ is small (in which case the function is resilient with low order and has almost optimum nonlinearity). This comes from the fact that Kerdock codes and Preparata codes are rather extremal codes, considering their cardinalities, minimum distances, dual distances, and covering radii. This is still the case of the other known sequences of nonlinear codes listed at Subsection

5.5.2. It would be interesting to investigate (infinite classes of) nonlinear systematic codes with minimum distances and dual distances near each other, and with cardinalities and covering radii large enough.

## ACKNOWLEDGMENTS

We thank Iwan Duursma for helpful information.

Received March 4, 1988; final manuscript received September 8, 1998

## REFERENCES

1. Baker, R. D., Van Lint, J. H., and Wilson, R. M. (1983), On the Preparata and Goethals codes, *IEEE Trans. Inform. Theory* **IT-29**, 342–345.
2. Bierbrauer, J., Gopalakrishnan, K., and Stinson, D. R. (1994), Bounds for resilient functions and orthogonal arrays *in* "Advances in Cryptology, CRYPTO'94," Lecture Notes in Computer Sciences, Vol. 839, pp. 247–256, Springer-Verlag, New York/Berlin.
3. Brouwer, A. E., and Tholhuizen, L. M. G. M. (1993), A sharpening of the Johnson bound for binary linear codes and the nonexistence of linear codes with Preparata parameters, *Designs Codes Cryptogr.* **3**, 95–98.
4. Camion, P., and Canteaut, A. (1996), Construction of $t$-resilient functions over a finite alphabet, *in* "Advances in Cryptology, EUROCRYPT'96," Lecture Notes in Computer Sciences, Vol. 1070, pp. 283–293, Springer-Verlag, New York/Berlin.
5. Camion, P., and Canteaut, A. (1996), Generalization of Siegenthaler inequality and Schnorr-Vaudenay multipermutations, *in* "Advances in Cryptology, CRYPTO'96" (N. Koblitz, Ed.), Lecture Notes in Computer Science, Vol. 1109, pp. 372–386, Springer-Verlag, New York/Berlin.
6. Camion, P., Carlet, C., Charpin, P., and Sendrier, N. (1992), On correlation-immune functions, *in* "Advances in Cryptology, CRYPTO'91," Lecture Notes in Computer Sciences, Vol. 576, pp. 86–100, Springer-Verlag, New York/Berlin.
7. Carlet, C. *Partially-bent functions*, (1993), "Designs Codes and Cryptography," **3**, 135–145; and Proceedings of CRYPTO' 92, *in* "Advances in Cryptology," Lecture Notes in Computer Science, Vol. 740, pp. 280–291, Springer-Verlag, New York/Berlin, 1993.
8. Carlet, C. (1996), Hyper-bent functions, *in* "PRAGOCRYPT'96," pp. 145–155, Czech Technical University, Prague.
9. Carlet, C. (1997), More correlation-immune and resilient functions over Galois fields and Galois rings, *in* "Advances in Cryptology, EUROCRYPT'97," Lecture Notes in Computer Science, Vol. 1233, pp. 422–433, Springer-Verlag, New York/Berlin.
10. Carlet C. (1998), On the propagation criterion of degree $\ell$ and order $k$, *in* "Advances in Cryptology, EUROCRYPT'98," Lecture Notes in Computer Science, Vol. 1403, pp. 462–474.
11. Carlet, C., Recent results on bent functions, *in* "Proceedings of International Conference on Combinatorics," Information Theory and Statistics, 1997, to appear.
12. Carlet, C. (1998), $\mathbf{Z}_{2^k}$-linear codes, *IEEE Trans. Inform. Theory* **44**, No. 4, 1543–1547.
13. Delsarte, P. (1973), An algebraic approach to the association schemes of coding theory, Thesis, Université Catholique de Louvain.
14. Delsarte, P. (1973), Four fundamental parameters of a code and their combinatorial significance, *Information and Control* **23**, 407–438.
15. Delsarte, P., and Goethals, J.-M. (1975), Alternating bilinear forms over $GF(q)$, *J. Combin. Theory Ser. A* **19**, 26–50.
16. Dillon, J. F. (1974), Elementary Hadamard Difference sets, Ph.D. Thesis, Univ. of Maryland.

17. Hammons Jr., A. R., Kumar, P. V., Calderbank, A. R., Sloane, N. J. A., and Solé, P. (1994), The $Z_4$-linearity of Kerdock, Preparata, Goethals and related codes, *IEEE Transactions on Information Theory* **40**, 301–320.
18. Hergert, F. B. (1990), On the Delsarte–Goethals codes and their formal duals, *Discrete Math.* **83**, 249–263.
19. Hirose, S., and Ikeda, K. (1994), "Nonlinearity Criteria of Boolean Functions," KUIS Technical Report, KUIS-94-0002.
20. Hirose, S., and Ikeda, K. (1995), Complexity of Boolean functions satisfying the propagation criterion, *in* "The Proc. of the 1995 Symposium on Cryptography and Information Security, SCIS95-B3.3."
21. Jakobsen, T., and Knudsen, L. R. (1997), The interpolation attack on block ciphers, *in* "Proc. of 4th Fast Software Encryption" (Eli, Biham, Ed.), LNCS, Vol. 1267, Springer-Verlag, New York/Berlin.
22. Knudsen, L. R. (1994), Truncated and higher order differentials, *in* "Proc. of 2nd Fast Software Encryption" (Bart Preneel, Ed.), LNCS, Vol. 1008, Springer-Verlag, New York/Berlin.
23. Kurosawa, K., and Satoh, T. (1997), Design of $SAC/PC(\ell)$ of order $k$ Boolean functions and three other cryptographic criteria, *in* " Advances in Cryptology, EUROCRYPT'97," Lecture Notes in Computer Science, Vol. 1233, pp. 434–449, Springer-Verlag, New York/Berlin.
24. Meier, W., and Staffelbach, O. (1990), Nonlinearity Criteria for Cryptographic Functions, *in* "Advances in Cryptology, EUROCRYPT'89," Lecture Notes in Computer Science, Vol. 434, pp. 549–562, Springer-Verlag, New York/Berlin.
25. Preneel, B., Van Leekwijck, W., Van Linden, L., Govaerts, R., and Vandevalle, J. (1991), Propagation characteristics of Boolean functions, *in* "Advances in Cryptology, EUROCRYPT'90," Lecture Notes in Computer Sciences, Vol. 473, pp. 161–173, Springer-Verlag, New York/Berlin.
26. Preneel, B., Govaerts, R., and Vandevalle, J. (1991), Boolean functions satisfying higher order propagation criteria, *in* "Advances in Cryptology, EUROCRYPT'91," Lecture Notes in Computer Sciences, Vol. 547, pp. 141–152, Springer-Verlag, New York/Berlin.
27. Preneel, B. (1993), Analysis and design of cryptographic hash functions, Ph.D. Katholieke Universiteit Leuven, U.D.C. 621.391.7.
28. Rothaus, O. S. (1976), On bent functions, *J. Combin. Theory Ser. A* **20**, 300–305.
29. Mac Williams, F. J., and Sloane, N. J. (1977), "The Theory of Error-Correcting Codes," North Holland, Amsterdam.
30. Stinson, D. R. (1993), Resilient functions and large sets of orthogonal arrays, *Congressus Numer.* **92**, 105–110.
31. Stinson, D. R., and Massey, J. L. (1995), An infinite class of counterexamples to a conjecture concerning nonlinear resilient functions, *Journal of Cryptology* **8**, 167–173.
32. Webster, A., and Tavares, S. (1985), On the design of S-boxes, *in* "Advances in Cryptology, CRYPTO'85," Lecture Notes in Computer Science, Vol. 218, pp. 523–534.
33. Xiao, Guo-Zhen, and Massey, J. L. (1988), A spectral characterization of correlation-immune combining functions, *IEEE Trans. Inf. Theory* **34**, 569–571.
34. Zhang, X.-M., and Zheng, Y. (1996), Characterizing the structures of cryptographic functions satisfying the propagation criterion for almost all vectors, *Designs, Codes and Cryptography* **7**, 111–134.